양자컴퓨터와 NIST 양자내성암호 표준화 동향

장경배*, 서화정*
*한성대학교 대학원 IT융합공학과
e-mail:starj1023@gmail.com

Quantum Computer and Standardization trend of NIST Post-Quantum Cryptography

Kyoung-Bae Jang*, Hwa-Jeong Seo*
*Dept. of Applied IT Engineering, Han-sung University

요 약

현재 양자컴퓨터 개발에 대한 전폭적인 연구가 이루어지고 있다. 지금의 양자컴퓨터의 개발수준은 기존 암호 시스템에 위협이 될 정도는 아니지만, 가까운 미래에 다가올 양자컴퓨터 시대에 대한 양자내성암호가 필요한 상황이다. 이에 양자내성암호 표준화를 위해 미국 NIST는 공모전을 열었고, 본 논문에서는 양자컴퓨터 개발현황과 NIST(National Institute of Standards and Technology) 양자내성암호 공모전의 암호알고리즘 설명과 동향을 살펴보고자 한다.

1. 서론

현재 양자컴퓨터가 국내외적으로 활발하게 연구되고 있다. 수학자 Shor는 양자컴퓨터를 사용하여 소인수분해 문제를 빠르게 해결할 수 있는 양자알고리즘을 개발하였다. 이 알고리즘은 소인수 분해 문제를 기반으로 한 몇몇 암호 시스템들을 더 이상 사용할 수 없게 만든다. 현재 널리 사용되고 있는 공개키 암호화 시스템인 RSA 또한 그 대상이다. 이 알고리즘이 실제로 적용가능한 수준의 양자컴퓨터가 개발되기 전에 양자컴퓨터의 계산능력에 내성을 가진 양자내성암호가 필요한 상황이다. 이에 본 논문에서는 양자컴퓨터의 개발현황에 대하여 설명한 뒤, NIST의 양자내성암호 표준화를 위한 공모전과 연관하여 양자내성암호에 대한 동향을 살펴보고자 한다.

2. 양자컴퓨터 시대

기존컴퓨터와 달리 양자컴퓨터는 양자 중첩, 양자 얽힘 등의 양자역학적 개념을 도입한 양자비트라 불리는 큐비트를 사용한다. 기존 컴퓨터가 0이나 1 중 하나로 비트상태를 결정했다. 하지만 큐비트는 0과 1을 동시에 가질 수 있는 상태로 존재하는데 이러한 성질을 양자 중첩이라고 한다. 하나의 큐비트가 여러 가지 정보를 표현할 수 있고 큐비트의 수가 늘어날수록 표현할 수 있는 정보의 양이 지수적으로 증가한다. 정보처리 관점에서 보면 엄청나게 큰 메모리 공간과 여러 가지 정보를 동시에 처리함으로써 병렬적인 연산이 가능하게 된다. 큐비트는 여러 정보를 가질 수 있는 상태로 존재하다가 관측되는 순간 그 상태가 결정된다. 양자얽힘이란 큐비트가 관측되었을 때, 관측된 큐비트와 얽혀있는 큐비트의 상태까지 결정되는 성질이다. 이 특징은 데이터가 순식간에 다른 곳으로 이동하는 것으로 보인다. 큐비트의 중첩과 얽힘의 성질을 사용한 양자컴퓨터는 기존컴퓨터에서는 빠르게 해결하지 못했던 분야에 대하여 엄청난 해결능력을 가지게 된다. 1994년 수학자 Shor는 소인수분해 시 주기성을 찾는 문제에 효율적인 양자 알고리즘을 제안하였다. 이 알고리즘을 구동할 수 있는 수준의 양자컴퓨터가 개발된다면 소인수분해 문제의 어려움을 기반으로 한 공개키 암호화 시스템은 더 이상 안전하지 않게 된다. 아직 그 수준에 도달하진 않았지만 2018년 3월 구글은 72 큐비트 양자컴퓨터 브리슬콘을 공개하였다. 구글 싱크탱크가 말한 양자컴퓨터가 기존 슈퍼컴퓨터의 성능을 뛰어넘는다는 50큐비트보다 큰 크기인 것이다. 하지만 큐비트를 이용한 연산과정에서는 주변 환경에 정말 미세한 노이즈만 있어도 실패하게 된다. 이러한 이유로 노이즈를 방지하기위해 초저온환경에서 연산을 수행하곤 한다. 이처럼 양자컴퓨터에 대한 과제는 그 크기를 늘리는 것뿐만이 아니라 오류율을 줄이는 단계에도 있으며 현재 글로벌 IT그룹인 구글, IBM 등 모두 양자컴퓨터 개발에 힘쓰며 가까운 미래에 도래할 양자컴퓨터 시대를 준비하고 있다.

3. 양자내성암호

양자컴퓨터에 대한 연구가 활발히 진행됨에 따라 양자컴퓨터의 계산능력에 내성을 가진 양자내성암호가 필요한 시점이다. 양자컴퓨터가 모든 수학적 분야에 대하여 기존컴퓨터보다 계산능력이 뛰어난 것은 아니기 때문에 새로운 수학적 문제에 기반 한 양자내성암호가 제안되고 있는 상황이다. 기존에 연산속도, 키 크기의 문제로 다른 암호

기법과 비교해 그 효율성이 떨어져 주목받지 못하던 암호 기법들이 양자컴퓨터에 대한 개발과 관심으로 인해 양자내성암호 후보군으로 떠오르게 되었다. 현재 양자컴퓨터의 공격에 안전하다고 여겨지는 암호기법은 격자기반 암호, 부호기반 암호, 다변수 다항식 기반 암호, 아이소제니 기반 암호 등이 있다. 이러한 암호들은 양자컴퓨터 뿐만이 아니라 기존컴퓨터의 공격에서도 그 안전성이 검증되었다. 하지만 앞서 언급하였듯 기존 암호에 비해 효율성이 떨어지기 때문에 안전하다 하더라도 양자내성암호에 대한 문제는 안전성과 효율성의 트레이드오프에 있다. 새로운 암호체계를 도입하기 위해선 개발, 협의, 표준화, 안전성검증 등의 이유로 오랜 시간이 소요된다. 그러므로 실제로 공격이 되기 전 미리 효율적인 방어시스템을 구축해야 할 필요가 있다. 암호시스템은 오래 유지될수록 그 안전성을 검증할 수 있는데 그 점에서 기존컴퓨터를 이용한 여러 가지 공격은 오래전부터 이루어져 왔기 때문에 그 안전성을 검증하는 기간이 길다. 즉, 오랜 기간 다양한 공격에 버텨왔기 때문에 그 신뢰도가 더 높다는 것이다. 하지만 양자컴퓨터 시대가 다가왔을 때 어떤 새로운 방식의 양자컴퓨터를 이용한 공격이 실행될 수 있을지는 아무도 모르기 때문에 다양한 공격 잠재성에 대비하여 양자내성암호에 대한 지속적인 안전성 검증과 효율성에 대한 보완은 계속 연구되어야 할 것으로 보인다.

4. NIST 양자내성암호 표준화 공모전

미국 국립표준기술연구소 NIST 에서는 다가올 양자컴퓨터 시대를 대비하여 양자내성암호 표준화를 위한 공모전을 주최하였다. 공모전에는 국제적으로 많은 암호알고리즘이 참가하였으며 Round 1 에서는 NIST가 제시한 성능조건을 만족하는 69개의 양자내성암호 알고리즘이 선정되었다. 2019년 1월 30일 표준화 단계가 Round 2 로 진행됨에 따라 암호알고리즘의 안전성과 실용성에대한 평가에 의해 69개에서 26개의 후보자로 좁혀졌다. 발표한 26개의 암호알고리즘과 사용기법은 공개키 암호/키 설정이 17개, 서명이 9개로 구성되어있다[표 1]. 공개키 암호/키 설정에 사용된 기법은 격자와 부호가 대부분이며 각각 9개와 7개로 그 주를 이루고 아이소제니 1개로 구성되어있다. 좁혀진 후보군에 대하여 NIST는 Round 2 평가기간이 시작되기 전에 알고리즘 제출자에게 최적화된 최신구현을 요구하였으며 가장 유망하다고 생각되는 몇몇 제출 알고리즘에서도 작은 결함이 확인될 수 있다고 발표하였다. 따라서 보안이나 효율성의 목적에서 제출된 알고리즘에 대한 작은 수정을 허용하며 입증 정당성과 함께 사소한 변경사항을 마감일인 2019년 3월 15일 까지 제출하도록 하였고 변경된 알고리즘에 대해 철저한 평가를 하겠다고 밝혔다[1]. 암호 알고리즘의 성능이 Round 2 에서는 더 큰 역할을 할 것 이므로 NIST는 다음과 같은 사항을 제출자에게 요구하였다. 요구사항에는 암호 알고리즘에 대한 최적화 구현이 포함되는데 마이크로아키텍처 최적화 구현을 강력히 권고하였다. 또한 다른 소프트웨어와 하드웨어에 대한 최적화 구현을 마이크로컨트롤러와 프로그래밍이 가능한 하드웨어 FPGA(Field Programmable Gate Array)를 예시로 들며 최적화된 구현을 장려하였다[1]. NIST의 Round 2 발표를 종합해 보았을 때, 좁혀진 후보군에서도 작은 결함이 발견될 수 있다는 사실에 대해서는 양자내성암호에 대한 안전성 증명은 역시나 과도기에 있으며 지속적인 검증이 필요할 것으로 보인다. 그리고 최적화 요구조건을 제시하였는데, 이는 현실 세계에서 통신하는 다양한 IoT(Internet of Things) 디바이스 및 소형 디바이스에 적용시키기 위한 효율적인 양자내성암호 시스템을 구축하여 실생활에 적용 가능한지 여부를 중요시 하는 것으로 보인다. 3장에서 언급한 양자내성암호의 뚜렷한 단점인 느린 연산속도나 큰 크기의 키 등에 대한 효율성 문제를 연산능력이 제한적인 디바이스에서 어떻게 해결할지, 그리고 안전성과 효율성 사이의 트레이드오프 문제를 어떻게 풀어낼지 또한 주목할 사항이다. 이에 NIST Round 2 공개키 암호알고리즘에 대해 유형별로 한가지 씩 살펴보며 최신 양자내성암호의 특성에 대해 알아보고자 한다.

<표 1> NIST 양자내성암호 Round 2

유형	공개키암호/키생성	서명
격자	CRYSTALS-KHYBER Frondose LAC Newcome **NTRU** NTRU Prime Round 5 SABER Three Bears	CRYSTALS-DILITHIUM FALCON qTESLA
부호	BIKE **Classic McEliece** HQC LEDAcrypt NTS-KEM ROLLO RQC	
해쉬		SPHINCS+
다변수다항식		GeMSS LUOV MQDSS Rainbow
아이소제니	**SIKE**	
제로지식증명		Picnic

4.1 NTRU

NTRU는 1996년 Hoffstein, Pipher, Silverman가 제안한 격자기반 공개키 암호시스템이다[2]. NTRU에 대해 설명하기에 앞서 격자기반 암호란 컴퓨터 과학자 Ajtai[3]에 의해 제안되었으며 격자는 주기적인 구조와 n차원 공간의 점들의 집합이며 즉, n선형 독립 벡터들의 집합으로 격자

가 생성된다. 격자기반 암호는 상대적으로 효율적인 구현과 엄청난 간결성뿐만이 아니라 worst-case hardness에 기반 하여 매우 강력한 안전성을 보증하며 양자컴퓨터에 대항한 안전성 까지 신뢰되고 있다[4]. 격자문제의 어려움 중 가장 기초는 임의로 표현된 격자가 주어지고 목표는 이 안에서 가장 짧은 0이 아닌 벡터를 찾아내는 SVP(Shortest Vector Problem) 이다. 이는 두 가지 추정에 의해 안전하다고 여겨지는데 첫 번째는 다항계수내의 격자문제에 대한 다항시간 알고리즘이 존재하지 않다는 것이다[5]. 격자문제에 대하여 여러 알고리즘을 적용시켜 보아도 가장 좋은 알고리즘은 지수적인 시간에 실행되거나 매우 나쁜 근사치의 결과를 보여주었다[6]. 두 번째는 격자문제를 효율적으로 해결하는 양자 알고리즘 또한 없다는 것이다[7]. 인수분해 시 주기성을 찾는 어려움에 사용되는 Shor의 양자 알고리즘은 격자문제에는 적합하지 않다. 이러한 이유로 격자기반암호의 사용이 양자내성암호의 역할을 할 수 있다고 말할 수 있다. NTRU는 인수분해나 이산로그 문제에 기반 하지 않은 최초의 공개키 암호화 시스템이다. NIST 양자내성암호 공모전 Round 2 에서 평가 대상이며 RSA를 대체할 수 있다고 주목받는 격자기반 암호화 시스템이다. 격자 안에서 가장 짧은 벡터를 찾는 문제(SVP)에 기반하고 다항환 상에서 그 연산이 이루어진다. 명백한 장점은 기본적인 산술 연산을 통한 효율적인 구현이다. 때문에 저 전력 하드웨어나 임베디드 시스템 어플리케이션 등에 적합하다고 평가된다[8, 9]. 이 점은 NIST 양자내성암호 공모전 Round 2 에서 발표한 IoT 소형디바이스에 적용하기위한 평가단계에서 강점을 가질 것으로 보인다. 하지만 여러 가지 가능한 공격에 대해 내성을 가지는 알고리즘 파라미터 설정이 요구된다. 알고리즘은 [그림 1]과 같다.

파라미터 : (N,p,q)
키 생성 : $f * f_p = 1(\mathrm{mod}\, p), \quad f * f_q = 1(\mathrm{mod} q)$
공개키 : $h = pf_q * g(\mathrm{mod} q)$
암호화 : $e = r * h + m(\mathrm{mod} q)$
복호화 : $f * e(\mathrm{mod} q) = a$
$a(\mathrm{mod} p) = b$
$f_p * b(\mathrm{mod} p) = m$

(그림 1) NTRU 알고리즘

키 생성 단계에서 임의로 선택된 N-1차의 다항식 g 그리고 다항식 f에 대한 모듈러 p, q의 역을 계산하여 f_p, f_q , g 를 개인키로 가지게 된다. 참고로 p는 작은 수를 사용하며 q는 p보다 더 큰 수를 가진다. 이렇게 자신이 가진 개인키를 사용하여 공개키를 h를 생성하고 자신의 메시지 m에 매우 작은 크기의 벡터 r을 조합하여 암호문 e를 전송한다. 마지막으로 암호문 수신자는 자신의 개인키를 이용하여 암호문에서 원본 메세지 m을 복구한다.

4.2 Classic McEliece

McEliece는 1978년 Robert J.McEliece에 의해 만들어진 부호이론을 이용한 공개키 암호시스템이다[10]. Shannon이 제안한 부호이론[11]의 핵심은 송신자는 부호에 작은 오류벡터를 추가하여 송신하게 되면 수신자가 자신이 가지고 있는 오류수정부호를 사용하여 정상부호를 획득하는 것이다. 이 기법은 McEliece 공개키 암호시스템에서도 유용하게 사용되는데, 부호는 선형 오류수정 부호인 Goppa 부호를 사용한다. 송신자는 부호를 이용한 공개키와 자신이 보낼 메시지를 조합한 뒤, 의도적으로 오류를 추가한 암호문을 송신한다. 그리고 수신자는 자신이 가지고 있는 오류수정부호를 사용하여 암호문을 해독한다. 암호문을 누군가 가로채도 오류수정부호를 알지 못하면 원본 메세지를 획득할 수 없기 때문에 공개키 암호시스템에 적합하다. 하지만 이때까지 매우 큰 키 크기 때문에 효율성이 떨어져 주목받지 못하였다. 하지만 양자컴퓨터가 개발됨에 따라 양자내성암호의 역할을 할 수 있을 것이라 주목받고 있다. McEliece는 초기에 알고리즘 파라미터의 수정은 있었지만 40년 동안 그 체계를 유지했다는 점에서 안전성이 더욱 보증되며, 양자컴퓨터 상에서도 또한 동일하다. 앞서 말한 매우 큰 크기의 키는 해결해야할 과제이며, 키 크기를 줄이는 등 효율성을 개선시키는 McEliece의 변형암호에 대한 연구[12] 또한 이루어지고 있다. McEliece의 알고리즘은 [그림 2]와 같다.

파라미터 : (n,t)
키 생성 : 주어진 파라미터를 이용
G: $k \times n$ 이진생성행렬, 고파부호
S: $k \times k$ 임의의 이진가역행렬
P: $n \times n$ 임의의 순열행렬
공개키 : $G' = SGP$
암호화 : $c = mG' \oplus e$
복호화 : $cP^{-1} = (mS)G \oplus eP^{-1}$
복호알고리즘 D_g 적용, $mSG = D_g(cP^{-1})$
마지막으로 G^{-1}, S^{-1}을 계산하여 m 획득

(그림 2) McEliece 알고리즘

Goppa부호를 사용하여 t개의 오류수정능력을 가진 행렬 G와 임의로 선택된 행렬 S, P를 개인키로 가지게 된다. 개인키를 조합하여 공개키 G'를 생성하고 송신자는 공개키와 자신의 메시지를 조합한 뒤, 오류 e를 더한 암호문 c를 전송한다. 암호문을 받은 수신자는 자신의 개인키와 G에 대한 효율적인 복호알고리즘을 적용하여 원본 메세지 m을 획득한다.

4.3 SIKE

현재 널리 사용되고 있는 타원곡선 암호 ECC(Elliptic Curve Cryptography)는 타원곡선 E에서의 입력 포인트 $P1$, $P2$ 의 숨겨진 관계의 이산대수문제에 기반 한다. ECC는 뛰어난 효율성을 자랑하여 메모리나 연산기능이 제한적인 다양한 IoT 제품에서 사용되었지만 소인수 분해와 이산대수 문제를 효율적으로 풀어내는 Shor 알고리즘을 이용한 양자컴퓨팅 공격에 그 취약함[13]이 드러났다. 대규모 IoT 제품의 무선통신이 오가는 4차 산업혁명 시대에 통신을 보안할 수 있는 양자내성암호가 필요한 상황[14]이다. SIKE는 NIST 양자내성암호 공모전 Round 2 에서 살아남은 유일한 아이소제니 기반 암호이다. 기존 타원곡선 기반 문제가 양자컴퓨터의 공격에 취약한 반면 SIKE는 Supersingular 타원곡선 상에서 연산이 이루어진다는 차별화로 양자컴퓨터의 공격에 내성을 가진다[15, 16]. 그리고 다른 양자내성암호 후보군들과 비교해 가장 짧은 키 크기로 동일한 안전성을 제공하기 때문에[17] Round 2 의 중요 평가기준인 효율성면에서 격자기반 암호와 같이 강점을 가질 것으로 보인다. 하지만 다른 암호들과 비교해보았을 때 등장한 지 얼마 되지 않은 암호이기에 사람들에게 익숙하지 않고 역사가 짧은 만큼 그 암호에 대한 검증기간도 짧다. 그러므로 안전성 측면에서는 더 지켜보아야 할 것으로 보이지만 뛰어난 성능을 가지고 있어 떠오르는 양자내성암호 후보군 중 하나이다.

5. 결론

양자컴퓨터 개발에 따른 기존 암호체계의 위협으로 인해 양자내성암호가 필요한 상황, 이에 NIST는 양자내성암호 공모전을 열었고 제안된 후보군들은 모두 다른 특성을 가지고 있다. NIST는 여러 개의 암호 알고리즘을 표준화할 가능성이 있다고 밝혔고[15] 구현환경이 제한적인 소형 디바이스에 적합한 암호 혹은 복잡한 연산이 가능한 PC에 적합한 암호 등 다양한 분야에 맞춰 하나이상의 양자내성암호가 표준화될 것으로 보인다. 이렇게 어떤 양자내성암호 후보군이 새로운 암호체계 구축의 일원이 될지 관심이 쏟아지고 있으며 그에 따른 NIST의 양자내성암호 표준화 공모전의 행보 또한 주목되어지는 상황이다. 앞서 언급하였듯 양자내성암호의 역할을 할 것이라 뽑히는 암호들이 모두 완벽한 상태는 아니다[1]. 하지만 이점은 양자컴퓨터도 똑같은 상황이기 때문에 현재 암호학계는 진화하는 양자컴퓨터에 대비한 암자내성암호에 관심과 노력이 활발히 이루어지고 있는 상황이며 그에 따라 안정적인 양자내성 암호체계에 구축에 대한 노력이 필요하다.

참고문헌

[1] NIST PQC team “Guidelines for submitting tweaks for 2nd Round candidates”

[2] J. Hoffstein, J. Pipher, and J. H. Silverman “NTRU: A Ring Based Public Key Cryptosystem”

[3] Ajtai, M.: Generating hard instances of lattice problems. In Complexity of computations and proofs, volume 13 of Quad. Mat., pages 1 – 32. Dept. Math., Seconda Univ. Napoli, Caserta (2004). Preliminary version in STOC 1996.

[4] Daniele Micciancio, Oded Regev “Lattice-based Cryptography”

[5] Oded Regev “On the Complexity of Lattice Problems with Polynomial Approximation Factors”

[6] Nicolas GamaPhong, Q. Nguyen “Predicting Lattice Reduction”

[7] Daniel J. Bernstein · Johannes Buchmann Erik Dahmen “Post-Quantum Cryptography”

[8] Manifavas C, Hatzivasilis G, Fysarakis K, Rantos K. “Lightweight cryptography for embedded systems – a comparative analysis“

[9] Hu F, Wilhelm K, Schab M, Lukowiak M, Radziszowski S, Xiao Y. “NTRU-based sensor network security: a low-power hardware implementation perspective”

[10] RJ McEliece, “A public-key cryptosystem based on algebraic”

[11] CE Shannon “A mathematical theory of communication”

[12] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, Paulo S. L. M. Barreto “MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes”

[13] Donny Cheung, Dmitri Maslov, Jimson Mathew, Dhiraj K. Pradhan “On the Design and Optimization of a Quantum Polynomial-Time Attacke on Elliptic Curve Cryptography”

[14] Chi Cheng, Rongxing Lu, Albrecht Petzoldt, and Tsuyoshi Takagi “Securing the Internet of Things in a Quantum World“

[15] David Jao, Luca De Feo “Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies”

[16] Craig Costello, Patrick Longa, and Michael Naehrig “Efficient algorithms for supersingular isogeny Diffie-Hellman“

[17] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon ,David Cooper ,Quynh Dang, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone “Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process“